(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－231773

(43)公開日　平成11年(1999)８月27日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６１０	Ｇ０９Ｃ　1/00	６１０Ｚ

審査請求　未請求　請求項の数７　ＯＬ　（全　７　頁）

(21)出願番号　特願平10－28877

(22)出願日　平成10年(1998)２月10日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　高橋　勝己
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

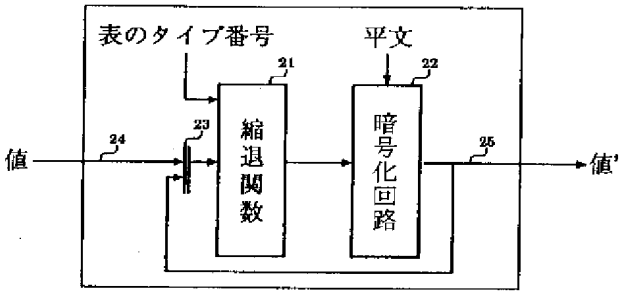
(74)代理人　弁理士　高田　守　（外１名）

(54)【発明の名称】　暗号強度評価装置

(57)【要約】

【課題】　メッセージ長が同一で鍵長や暗号化手法の異なる暗号に対し同一構成の装置により評価可能にして、装置の規模や実行時間を短く抑える暗号強度評価装置を提供する。

【解決手段】　表を作成するために初期値を与える手段４と、初期値を変形して表の要素を生成する手段５と、生成した表を格納する手段７と、入手した暗号文を取り込む手段１、４、９と、暗号文を変形して表の要素と比較する手段１１と、比較で一致したものが暗号文に対応する鍵であることを検証する手段１２、１３とからなり、前記暗号文を変形して表の要素と比較する手段は暗号文を変形して鍵を生成する鍵生成回路と、鍵を入力して暗号化する暗号化回路とを備えたＬＳＩ回路であり、ＬＳＩ回路を交換することにより、メッセージ長が同一であれば、鍵長や暗号化手法の異なる暗号に対しても同一構成の装置により暗号を評価可能にした。



1

【特許請求の範囲】

【請求項１】　平文を設定し、複数の表を作成するために初期値を与える手段と、初期値を変形して表の要素を生成する手段と、生成した表の要素を格納する手段と、入手した暗号文を取り込む手段と、表を取りだし暗号文を変形させて表の要素と比較する作業を繰り返す手段と、比較の結果一致したものが暗号文に対応する鍵であることを検証する手段とからなり、予め平文を想定して大量の表を作成し、暗号文入手後、その暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めることを特徴とする暗号強度評価装置。

【請求項２】　前記暗号文を変形させて表の要素と比較する作業を繰り返す手段は暗号文を入力して変形し鍵を生成する鍵生成回路と、前記鍵及び平文を入力して暗号化を行なう暗号化回路とを有するＬＳＩ回路からなることを特徴とする請求項１記載の暗号強度評価装置。

【請求項３】　前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵を生成する鍵生成回路に交換することにより、メッセージ長が同じで鍵長の異なる暗号を評価するようにしたことを特徴とする請求項２記載の暗号強度評価装置。

【請求項４】　前記鍵を入力して暗号化を行なう暗号化回路を他の暗号を行なう暗号化回路に交換することにより、メッセージ長が同一の他の暗号を評価するようにしたことを特徴とする請求項２または３記載の暗号強度評価装置。

【請求項５】　前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵の一部を変数として外部から受けとる回路に交換することにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたことを特徴とする請求項２記載の暗号強度評価装置。

【請求項６】　前記暗号文を変形し、鍵を生成する鍵生成回路に拡大転置を採用することによって、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたことを特徴とする請求項２記載の暗号強度評価装置。

【請求項７】　前記平文を入力して暗号化を行なう暗号化回路を複数設け、前記複数の暗号化回路のそれぞれに異なる平文を入力して暗号化し、前記鍵生成回路にその複数の暗号文を入力して鍵を生成するようにしたことにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたことを特徴とする請求項２記載の暗号強度評価装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、予め平文を想定し、暗号文に対応する鍵を探索することで暗号の強度を評価する暗号強度評価装置に関する。

【０００２】

2

【従来の技術】予め表を作成し、暗号文を加工しつつ表との比較を繰り返す暗号強度評価は、『M.E.Hellman, "A cryptanalytic time-memory trade-off", IEEETransaction on Infomation Theory, Vol.IT-26 No.4』という論文に述べられている。ここで、暗号の強度とは、暗号を解くために要するコスト（例えば、装置の大きさや解読時間など）であり、従って、暗号強度を評価するということは、暗号解読の結果そのコストを評価するということになる。

【０００３】

【発明が解決しようとする課題】しかしながら、この論文では暗号強度評価の手法が述べられているだけであり、この装置を構成する方法、すなわち、この手法を実現した装置または実現する手段については述べられていない。

【０００４】本発明は、上記従来の問題を解決するためになされたもので、上記論文に基づく手法を実現するための手段を提供し、特にメッセージ長が同一であり、鍵長や暗号化手法の異なる暗号に対し同一構成の装置により評価可能にして、装置の規模や実行時間を短く抑えるようにした暗号強度評価装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】請求項１にかかる発明における暗号強度評価装置は、平文を設定し、複数の表を作成するために初期値を与える手段と、初期値を変形して表の要素を生成する手段と、生成した表の要素を格納する手段と、入手した暗号文を取り込む手段と、表を取りだし暗号文を変形させて表の要素と比較する作業を繰り返す手段と、比較の結果一致したものが暗号文に対応する鍵であることを検証する手段とからなり、予め平文を想定して大量の表を作成し、暗号文入手後、その暗号文の加工と前記表との比較を繰り返しながら、暗号文の鍵を求めるようにしたものである。

【０００６】請求項２にかかる発明における暗号強度評価装置は、前記暗号文を変形させて表の要素と比較する作業を繰り返す手段は暗号文を入力して変形し鍵を生成する鍵生成回路と、前記鍵及び平文を入力して暗号化を行なう暗号化回路とを有するＬＳＩ回路からなるようにしたものである。

【０００７】請求項３にかかる発明における暗号強度評価装置は、前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵を生成する鍵生成回路に交換することにより、メッセージ長が同じで鍵長の異なる暗号を評価するようにしたものである。

【０００８】請求項４にかかる発明における暗号強度評価装置は、前記鍵を入力して暗号化を行なう暗号化回路を他の暗号を行なう暗号化回路に交換することにより、メッセージ長が同一の他の暗号を評価するようにしたものである。

【０００９】請求項５にかかる発明における暗号強度評価装置は、前記暗号文を変形し鍵を生成する鍵生成回路を他の鍵長の鍵の一部を変数として外部から受けとる回路に交換することにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたものである。

【００１０】請求項６にかかる発明における暗号強度評価装置は、前記暗号文を変形し鍵を生成する鍵生成回路に拡大転置を採用することによって、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたものである。

【００１１】請求項７にかかる発明における暗号強度評価装置は、前記平文を入力して暗号化を行なう暗号化回路を複数設け、前記複数の暗号化回路のそれぞれに異なる平文を入力して暗号化し、前記鍵生成回路にその複数の暗号文を入力して鍵を生成するようにしたことにより、メッセージ長が同じで、鍵長がメッセージ長を越える他の暗号を評価するようにしたものである。

【００１２】

【発明の実施の形態】以下、添付図面、図１乃至図３に基づき、本発明の一実施の形態を詳細に説明する。図１は本発明の一実施の形態における暗号強度評価装置の構成を示すブロック図、図２は図１に示す暗号強度評価装置において暗号化の処理を行なうＬＳＩの詳細を示す構成図、図３は図２に示す暗号化回路を複数設けたＬＳＩの詳細を示す構成図である。

【００１３】実施の形態１．まず、図１を参照して、本発明の実施の形態における暗号強度評価装置の構成を説明する。以下、本実施の形態では、ＤＥＳという暗号を例に用いて説明する。ＤＥＳは、鍵長５６ビット，　メッセージ長（ 平文や暗号文の長さ）６４ビットとする暗号である。

【００１４】図１において、１は装置全体の管理やユーザとのインターフェイスを担うローカルコンピュータ、２ａ、２ｂはローカルコンピュータ１からの指示で処理を行なうそれぞれ一纏めにまとめたユニットであり、３はローカルコンピュータ１と各ユニット２ａ、２ｂとの間でデータの送受信を行なうためのネットワーク、４はユニット２ａ、２ｂ内全体を管理する制御用プロセッサであり、内部にローカルメモリーを有する。

【００１５】また、５ａ、５ｂは事前処理（暗号文作成のための表を作成する処理）において、初期値から暗号解読のための表の要素を作成する処理（暗号化処理、後述する）を行なうＬＳＩ　、６はデータを送受信のためのバス、７は表などを蓄える記憶装置、８ａ、８ｂは解読処理において値の検索を行なう検索ブロック、９は表の要素の検索を制御するプロセッサ、１０は表などを展開するメモリー、１１は暗号文を加工し変形させる（暗号化処理、後述する）ためのＬＳＩであり、検索ブロック８ａ、８ｂはこれらプロセッサ９、メモリー１０、ＬＳＩ１１から構成される。１２は検索ブロックが求めた解の候補を検証する検証用プロセッサであり、１３は検証用プロセッサ１２が検証する際に、値を加工する（暗号化処理、後述する）ＬＳＩである。

【００１６】尚、本実施の形態において、制御用プロセッサ４により平文を設定し、複数の表を作成するために初期値を与える手段を構成し、ＬＳＩ５ａ、５ｂにより初期値を変形して表の要素を生成する手段を構成し、記憶装置７により生成した表の要素を格納する手段を構成し、ローカルコンピュータ１、制御用プロセッサ４、プロセッサ９により入手した暗号文を取り込む手段を構成し、ＬＳＩ１１により表を取りだし暗号文を変形させて表の要素と比較する作業を繰り返す手段を構成し、検証用プロセッサ１２及びＬＳＩ１３により比較の結果一致したものが暗号文に対応する鍵であることを検証する手段を構成する。

【００１７】次に、図２を参照して、図１に示す暗号強度評価装置において暗号化の処理を行なうＬＳＩの詳細な構成を説明する。すなわち、図２に示すＬＳＩは、基本的には、図１に示すＬＳＩ５、２２、２３の全てに適用されるものである。しかし、違いとしては、ＬＳＩを使用している部所の役割りに応じて暗号化処理の反復回数が異なるよう動作することである。

【００１８】図２において、２１は縮退関数によって暗号文を変形し鍵を生成する鍵生成回路としての縮退関数回路（単に、縮退関数ともいう）、２２は縮退関数２１で変形された値を鍵として暗号化を行なう暗号化の回路または暗号化回路、２３は６４ビットの２入力１出力のセレクタである。セレクタ２３は外部からの初期値と内部でループする際の値を切替える。２４は縮退関数２１に対して入力する６４ビットのデータ線、２５は暗号化回路２２から出力する６４ビットのデータ線である。

【００１９】次に、図１及び図２を参照して、本発明の実施の形態における暗号強度評価装置の動作を説明する。本実施の形態における動作を、暗号文入手前にその解読のための表を作成する事前処理と、暗号文入手後にその表を用いて解読する解読処理及び解読の結果を評価する評価処理（評価処理を解読処理に含めて解読処理ともいう）との２つに分けて説明する。また、ここでいう事前処理は暗号解読のための表を作成して記憶手段に格納する処理をいう。

【００２０】まず、事前処理は次のような処理手順で行なわれる。

(1) ローカルコンピュータ１は、ユーザの指示に従い平文などの処理に必要なパラメータを決定する。

【００２１】(2) ローカルコンピュータ１は、表作成の処理を各ユニット２ａ、２ｂに分配する。この時、ローカルコンピュータ１は、ネットワーク３を介し、平文、作成する表のタイプ（ 表タイプ番号１００番から２００番など）、表の要素数Ｍ及び表作成のための加工繰り返

し数Ｔ等をパラメータとして各ユニット２ａ、２ｂ内の制御用プロセッサ４へ送る。

【００２２】(3) 制御用プロセッサ４は、平文、表のタイプ、初期値及び加工繰り返し回数Ｔ等といったパラメータをＬＳＩ５ａ、５ｂへ送り、表の要素の作成を指示する。この時、初期値は、表のタイプと作成する要素の表での指標値（インデックス(index) 番号）から生成する。例えば、その初期値の値は、『表のタイプ番号 << log(Ｍ) + 指標値』で作成することができる。

【００２３】(4) 各ＬＳＩ５ａ、５ｂは、平文と初期値を入力として、指定された表のタイプに応じた処理を行ない新しい値を生成する。ＬＳＩ５ａ、５ｂは内部ループを持ち、この値を初期値の代わりに用いて、更に新しい値を生成するこれをＴ回数繰り返す。この後、各ＬＳＩ５ａ、５ｂは要素作成が終了した後、制御用プロセッサ４にその終了報告を行なう。

【００２４】(5) 制御用プロセッサ４は、終了報告を受けとった後、作成した値をＬＳＩ５ａ、５ｂから取りだし、次の表の要素作成を各ＬＳＩ５ａ、５ｂに指示する。この指示は、制御用プロセッサ４の処理が終了するまで繰り返される。

【００２５】(6) 制御用プロセッサ４は、表の全ての要素を受けとると、バス６を介して、その表を記憶装置７に書き込む。この時、表の各要素から、その作成に用いられた初期値を求めるのに必要な情報も合わせて格納する。これを全ての表を作成するまで繰り返す。

【００２６】(7) 制御用プロセッサ４は、全ての表の作成が終了すると、その旨をローカルコンピュータ１に報告する。

(8) ローカルコンピュータ１は、全てのユニット２ａ、２ｂから終了報告を受けとるまで待つ。以上の動作で、事前処理は終了する。

【００２７】次に、解読処理は次のような処理手順で行なわれる。

(1) ローカルコンピュータ１に暗号文が入力される。

(2) ローカルコンピュータ１は、暗号文をネットワーク３を介して各ユニット２ａ、２ｂの制御用プロセッサ４へ送る。

【００２８】(3) 制御用プロセッサ４は、暗号文を検索ブロック８ａ、８ｂの全てに送った後、記憶装置７から表を取り出して各検索ブロック８ａ、８ｂに配布する。

(4) 検索ブロック８ａ、８ｂのプロセッサ９は、暗号文と表を受けとると、それをメモリー１０に格納する。

【００２９】(5) プロセッサ９は、入手した暗号文と表の各要素（暗号化したもの）との比較を行なう。比較した際、表の要素の中に一致するもの（解読したことになる）があれば、その要素の指標から、その要素が生成される際に用いられた初期値を求める。

【００３０】(6) (5) で表の要素と一致しなかった場合、プロセッサ９は、ＬＳＩ１１に対し暗号文を入力して処理させ、表から新しい値を取り出して、更に表の各要素との比較を行なう。表の要素の中に一致するものがあれば、その要素の指標から、その要素が生成される際に用いられた初期値を求める。一致するものがあった場合には、下記(17)の処理に移る。

【００３１】(7) プロセッサ９は、(6) 項における比較結果の如何に拘らず、ＬＳＩ１１が処理してできた新しい値を入力として更に処理させ、それによってできた新しい値を取り出して、表の各要素との比較を行なう。表の要素の中に一致するものがあった場合には、その要素の指標から、その要素が生成される際に用いられた初期値を求める。

【００３２】(8) 事前処理において加工を繰り返し行なった回数Ｔだけ(7) 項の処理を繰り返す。

(9) プロセッサ９は、(6) ～(8) 項の処理結果について一致した値の有無と、一致した場合の対応する初期値と、それが (6)の処理を１回目として何回目の加工だったかという情報とを制御用プロセッサ４に報告する。

【００３３】(10) 制御用プロセッサ４は、一致した値が報告された場合、その初期値、検索における加工回数、平文、表のタイプ番号及び表作成時の加工回数Ｔを検証用プロセッサ１２に送る。また、制御用プロセッサ４は、一致した値の有無に拘らず、記憶装置７から他の表を取り出し、ブロック８ａ、８ｂに同様の処理を指示する。この作業は、全ての表に対する処理が終了するまで繰り返される。

【００３４】(11) 検証用プロセッサ１２は、表作成時に行なわれた加工回数Ｔから比較処理で一致するまでに、ＬＳＩ１１が処理した回数を引いた値を求め、この値、初期値、平文及び表のタイプ番号をＬＳＩ１３に送る。

【００３５】(12) ＬＳＩ１３は、上記 (11) 項で減算した値と、初期値、平文及び表のタイプ番号とを受けとり、指定した回数、及び、その回数よりも１回少ない回数処理した結果（暗号の解読結果である鍵を生成するために必要）の２つを検証用プロセッサ１２に送る。

【００３６】(13) 検証用プロセッサ１２は、ＬＳＩ１３から受けとった値のうち、指定した回数処理した結果を入手した暗号文と比較する。ここで、値が一致した場合は、１回分処理の少ない値を入力して縮退関数の値を求め、それを解読結果（鍵）だとして、制御用プロセッサ４に報告する。

【００３７】(14) 制御用プロセッサ４は、解読結果を受けとった場合、ネットワーク３を介してその値をローカルコンピュータ１に報告する。一方、終了報告を受けとった場合には、他の検証すべき値を検証用プロセッサ１２に送る。

【００３８】(15) 制御用プロセッサ４は全ての表の処理が終了した場合、ローカルコンピュータ１に対して、その終了報告を行なう。

(16) ローカルコンピュータ１は、解読結果（鍵）を受けとった場合、その値を表示すると共に、各ユニット２ａ、２ｂに対し処理の中止を指示する。また、解読結果を受けとらず、全てのユニット２ａ、２ｂから終了報告を受けとった場合、鍵が発見できなかった旨を表示する。

【００３９】(17) 制御用プロセッサ４は、(5) において一致した値が報告された場合、表作成時の加工回数Ｔから１を引いた値、一致した要素に対応する初期値、平文及び表のタイプ番号を検証用プロセッサ１２に送る。検証用プロセッサ１２は、これらの値をＬＳＩ１３に転送する。ＬＳＩ１３は、初期値、平文及び表のタイプ番号を受けとり、その処理を指定されたＴ－１回繰り返す。検証用プロセッサ１２は、ＬＳＩ１３から処理結果の値を受けとり、この値を縮退関数の引数として関数の値を求め、これを解読結果（鍵）だとして制御用プロセッサ４に報告する。制御用プロセッサ４は、解読結果を受けとった場合、その値をローカルコンピュータ１にネットワーク３を介して報告する。ローカルコンピュータ１は、解読結果（鍵）を受けとった場合、その値を表示すると共に、各ユニット２ａ、２ｂに対し処理の中止を指示する。以上で、解読処理動作を終了する。

【００４０】実施の形態２．以下、図２を参照して、実施の形態２、３、４及び５における暗号化の処理について説明する。暗号化回路２２は、５６ビットの鍵を要求するため、縮退関数２１は入力した暗号文６４ビットから５４ビットへの変換とその値の変形とを実行する。暗号化回路２２が５６ビットを越える鍵を要求する場合は、取り除くビット数を減らした縮退関数（鍵生成回路）に交換する、すなわち、ＬＳＩを交換することによって、鍵長の異なる暗号に対応させることができるようにした。

【００４１】実施の形態３．実施の形態２においては、図２に示す暗号化回路２２は、ＤＥＳの暗号化を行なうようにしたが、実施の形態３においては、これを他の暗号化回路に変える、すなわち、ＬＳＩを交換することによって、異なる暗号（例えば、ＤＥＳ、ＦＥＥＬ）に対応することができるようにした。

【００４２】実施の形態４．実施の形態２においては、図２に示す縮退関数２１は、ビット数の削減とその値の変換とを行なうものとした。そのため、縮退関数２１は、メッセージ長を越える鍵長を生成することができなかった。しかし、鍵長がメッセージ長を越える場合、暗号文を変形し鍵を生成する回路を他の鍵長の鍵の一部を変数として外部から受けとる回路に交換して、別途外部から値を取り込むようにすることによって、メッセージ長を越える鍵長に対応させることができる。この外部から取り込む値は、装置の利用者もしくは装置自体が定数として与える方法がある。また、表の初期値と同様に、表の要素番号、表のタイプ番号及び縮退関数と、暗号化を繰り返した回数等といった値を引数とした関数値を与える方法もある。この関数値としてもっとも簡単なものは、引数をそのまま関数値として返す関数である。すなわち、このように、ＬＳＩを交換することによって、メッセージ長ビット以上の鍵長のものに対応するようにした。

【００４３】尚、メッセージ長の方が大きい場合には、１つの暗号文だけでは、鍵を特定することはできない。このため、もう１つ別の平文とその暗号化の結果である暗号文が必要になる。この場合、２つの平文に対し、生成した２つ暗号文が、両方とも、入手した２つの暗号文と一致した場合にのみ、それが鍵であると見做される。

【００４４】実施の形態５．実施の形態４においては、鍵長がメッセージ長を越える場合、不足分を開部からの入力で賄うようにしたが、ＤＥＳの内部処理で行なっているような、暗号文を変形し鍵を生成する回路に拡大転置を用いてビット長を増やす方法がある。このように、ＬＳＩを交換することによって、メッセージ長ビット以上の鍵長のものに対応するようにした。尚、拡大とはビット数を増やすこと、転置とはビットを入れ換えることである。

【００４５】実施の形態６．次に、図３を参照して、複数の平文を用いて暗号化を処理するＬＳＩについて説明する。実施の形態４及び５においては、平文を１つとして処理を行なうようにしたが、本実施の形態では、その平文を複数に増やすことによって不足分を補う方法を採用する。

【００４６】図３において、３１は縮退関数によって暗号文を変形し鍵を生成する鍵生成回路としての縮退関数回路（単に、縮退関数ともいう）、３２は縮退関数３１で変形された値を鍵として暗号化を行なう暗号化回路、３３はセレクタである。すなわち、図３は、図２の暗号化回路を複数にしたものである。

【００４７】次に、図３を参照して、複数の平文を用いて暗号化を処理するＬＳＩの動作について説明する。縮退関数３１は、セレクタ３３の値と線３６の値を受けとり、鍵を生成する。セレクタ３３が線３４の値を選択する場合、暗号化回路３２ｂの出力である線３６の値は予め設定した値となる。ここで設定する値は通常０である。

【００４８】すなわち、本実施の形態においては、鍵長がメッセージ長を越える場合、複数の異なる平文を用意し、暗号文を変形し鍵を生成する回路に複数の暗号文を入力として与え、鍵を生成するよう、ＬＳＩを交換することによって、メッセージ長ビット以上の鍵長のものに対応するようにした。

【００４９】以上説明した図１乃至図３に示す回路はハードウェアにより実現されるが、ソフトウェアによって実現することも可能である。

【００５０】

【発明の効果】請求項１及び２にかかる発明は、上記のように構成し、特に処理の入出力をメッセージ長に合わせ、メッセージ長が同一であれば、ＬＳＩを交換するだけで同一構成の装置により、異なる鍵長または異なる暗号化手法に容易に対応して評価可能にしたことにより、暗号強度評価装置の規模や実行時間を短く抑えることができる暗号強度評価装置を提供することができる。

【００５１】請求項３にかかる発明は、上記のように構成し、特にＬＳＩを交換して鍵生成回路を変えることにより、メッセージ長ビット以下の鍵長の違うものに対応することができる。

【００５２】請求項４にかかる発明は、上記のように構成し、特にＬＳＩを交換して暗号化回路を異なる暗号のものに変えることにより、メッセージ長が同じ他の暗号に対応することができる。

【００５３】請求項５にかかる発明は、上記のように構成し、特にＬＳＩを交換して、暗号文を変形し鍵を生成する回路を他の鍵長の鍵の一部を変数として外部から受けとる回路にかえることにより、メッセージ長ビット以上の鍵長のものに対応することができる。

【００５４】請求項６にかかる発明は、上記のように構成し、特にＬＳＩを交換して、暗号文を変形し鍵を生成する回路に拡大転置を採用することにより、メッセージ長ビット以上の鍵長のものに対応することができる。

【００５５】請求項７にかかる発明は、上記のように構成し、特にＬＳＩを交換して、複数の異なる平文をそれぞれ入力して暗号化し、その複数の暗号文を入力して鍵を生成することにより、メッセージ長ビット以上の鍵長のものに対応することができる。

【図面の簡単な説明】

【図１】　本発明の一実施の形態における暗号強度評価装置の構成を示すブロック図、

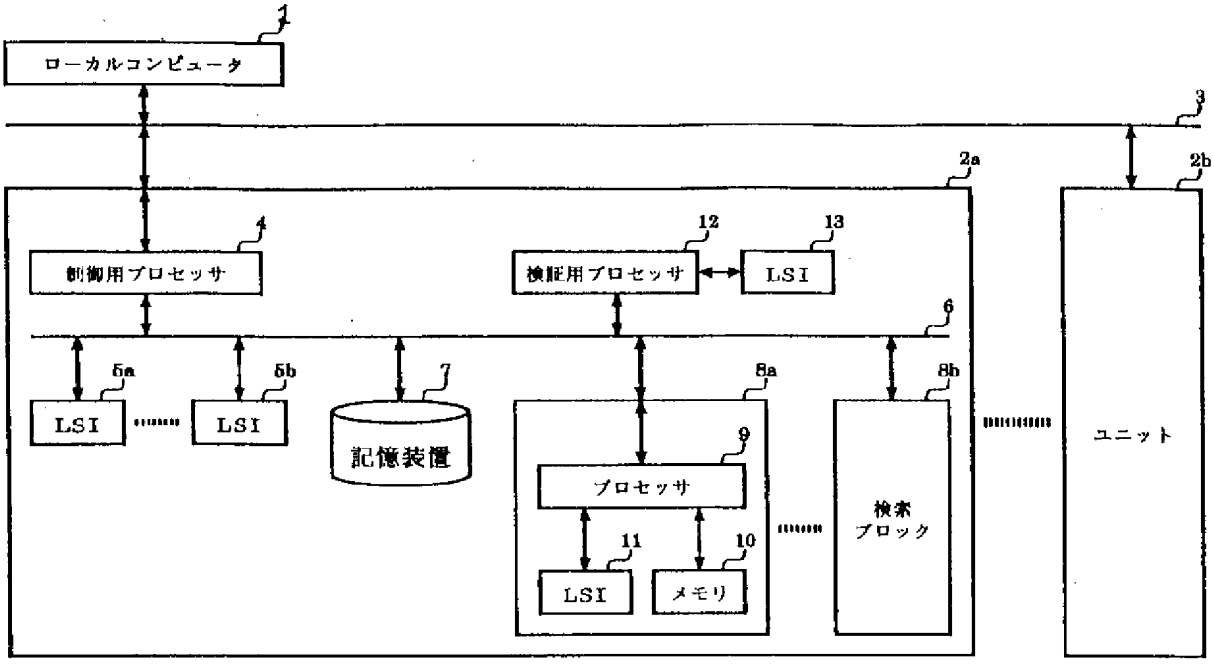
【図２】　図１に示す暗号強度評価装置において暗号化の処理を行なうＬＳＩの詳細を示す構成図、

【図３】　図２に示す暗号化回路を複数設けたＬＳＩの構成を詳細に示す図である。

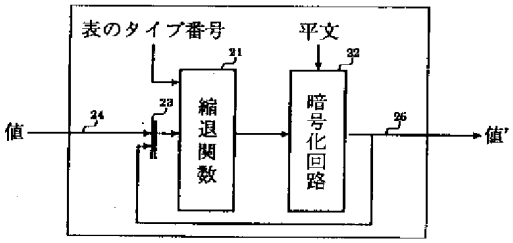
【符合の説明】

１　ローカルコンピュータ、　２ａ、２ｂ　ユニット、　３　ネットワーク、４　制御用プロセッサ、　５ａ、５ｂ　事前処理用ＬＳＩ、　７　記憶装置、６　バス、　８ａ、８ｂ　検索ブロック、　１２　検証用プロセッサ、９　検索用プロセッサ、　１０　メモリー、　３２ａ、３２ｂ　縮退関数回路、１１　解読処理における検索用ＬＳＩ、　１３　解読処理における検証用ＬＳＩ２１　暗号化回路、　２２　縮退関数回路、　２４、２５　外部との入出、２３　セレクタ、　３１　暗号化回路、　３３　セレクタ、３４、３５　外部との入出力線、　３６　暗号化回路３２ｂの出力線。

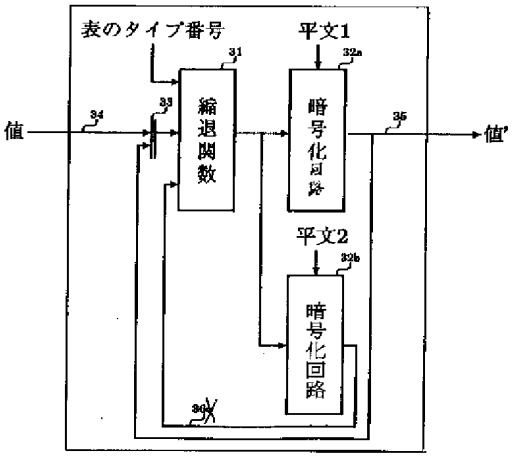
【図１】



【図２】


表のタイプ番号
平文
31
32
値
34
33
縮退関数
暗号化回路
36
値'

【図３】


表のタイプ番号
平文1
31
32a
値
34
33
縮退関数
暗号化回路
35
値'
平文2
32b
暗号化回路
30